ЛЕКЦИЯ

**По теме: «Профилактика и предупреждение преступлений в сфере информационно-телекоммуникационных технологий»**

В настоящее время увеличилось количество преступлений с использованием информационно-телекоммуникационных технологий, совершаемых следующими способами:

1) Киберпреступления, связанные с оформлением займов в микрофинансовых организациях на граждан третьими лицами, используя их персональные данные через портал Госуслуг, доступ к которому преступники получают при использовании кодов из смс-сообщений, которые граждане сообщают псевдо - сотрудникам сотовых компаний, пенсионного фонда и других структур, оказывающих услуги. Кроме того, доступ к порталу услуг мошенники могут получить используя старый абонентский номер, который был привязан ранее.

В указанных случаях необходимо немедленно прекратить разговор, позвонить по номеру «горячей линии» банковского учреждения, организации в сфере оказания социальных услуг, либо лично посетить офисы и поинтересоваться по поводу сомнительных манипуляций.

При прекращении пользования абонентским номером необходимо отвязать его от всех банковских приложений и личного кабинета портала Госуслуг.

2) Использование аккаунтов в мессенджерах, созданных от имени руководителей, для осуществления переписки, в ходе которой преступники просят перечислить деньги в долг на банковскую карту, либо оказать содействие правоохранительным органам в поимке преступников в банковской сфере. Далее, как правило, гражданину звонят неизвестные, представляющиеся сотрудниками силовых структур (ФСБ, МВД) и под предлогом его задействования в «спецоперации» по установлению преступников, убеждают оформить кредиты, снять личные сбережения и переводить деньги на подконтрольные им счета.

Если в мессенджере Вам написал руководитель и попросил деньги в долг, либо сказал, что с Вами должны связаться сотрудники правоохранительных органов и им необходимо помочь, а также неукоснительно выполнять их указания, не рискуйте, а просто перезвоните ему, либо свяжитесь другим удобным способом, который позволит понять, что с Вами на связи именно руководитель, а не преступник.

3) Взлом социальных сетей или аккаунтов в мессенджерах, и осуществление рассылки сообщений с просьбой одолжить денежные средства, либо перейти по ссылке и проголосовать за кого-либо.

4) Популярность в преступной среде набирает способ использования удалённого приобретения товаров в сети Интернет посредством приложений крупных торговых площадок (маркетплейсов).

Преступники, выступая в качестве продавцов, размещают объявление о продаже различного товара по выгодней цене. После оформления покупателем, доставка выбранного товара в указанный срок в пункт выдачи умышленно не осуществляется, в связи с чем покупатель вынужден обратиться в адрес технической поддержки маркетплейса с претензией о возврате товара, о чем сообщается недобросовестному продавцу.

В ходе разбирательства по неисполнению денежно-товарных обязательств псевдо-продавцы инициативно выходят на связь с покупателем и предлагают отменить ранее сделанный заказ (так как возникли технические проблемы на сайте «OZON») и осуществить новый.

Покупатели в мессенджере «Telegram» проходят по предоставленной им ссылке и попадают на «фишинговый» сайт «OZON», где осуществляют оплату товара, тем самым лишаются денежных средств.

5) Среди потерпевших от действий мошенников нередко становятся дети. Играя в онлайн-приложении на телефоне, подростки в чате получают различные сообщения, связанные с улучшением качества игры. Затем в переписке дети рассказывают о том, с кем они сейчас находятся и есть ли у них доступ к телефонам взрослых. Далее их убеждают продиктовать конфиденциальные данные, которые поступили на телефонные номера родственников. После чего происходит списание денежных средств.

Необходимо довести до детей информацию о различных уловках мошенников, в том числе о схемах, где под разным предлогами злоумышленники побуждают их сообщать конфиденциальную информацию взрослых, например, реквизиты банковских карт.

**Будьте бдительны и осторожны! Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 или 102 (с мобильных средств связи).**

«31» августа 2026 года